Lemma 7.3 If $K \subseteq L$ is a field ext., there is a group hom.

$$r_{L/K}: Br(K) \to Br(L), \quad [R] \mapsto [R \otimes_K L] \qquad (\text{"restriction"})$$

If $K \subseteq M \subseteq L$ are fields, $r_{L/K} = r_{L/M} \circ r_{M/K}$.

Proof: $R \otimes_K L$ is an L-CSA by [T6.3], [T6.4].

If $R \sim R'$, then $R \cong M_r(D)$, $R' \cong M_{r'}(D)$, so

$$R \otimes_K L \cong M_r(D) \otimes_K L \cong (D \otimes_K M_r(K)) \otimes_K L \overset{[P6.2(2)]}{\cong} (D \otimes_K L) \otimes_L (M_r(K) \otimes_K L)$$
$$\cong (D \otimes_K L) \otimes_L M_r(L).$$

Similarly $R' \otimes_K L \cong (D \otimes_K L) \otimes_L M_{r'}(L)$, so $R \otimes_K L \sim R' \otimes_K L$ (as L-CSAs)

Now $(R \otimes_K S) \otimes_K L \cong (R \otimes_K L) \otimes_L (S \otimes_K L)$ by [P6.2(2)], so $r_{L/K}$ is a group hom. □

7.1 Brauer group of $\mathbb{Q}$ (w/o proofs)

p-adic numbers: An absolute value on a field K is a map
$|\cdot| : K \to \mathbb{R}_{\geq 0}$ s.t. $\forall x, y \in K$:

(1) $|x| = 0 \Leftrightarrow x = 0$

(2) $|xy| = |x||y|$

(3) $|x+y| \leq |x| + |y|$

(Trivial if $|x| = 1 \ \forall x \neq 0$)

Then $d(x,y) := |x-y|$ is a metric on K, $+$ and $\cdot$ are continuous, so is inversion: $K^\times \to K^\times$, $x \mapsto x^{-1}$ (wrt. subspace topology).

K is a topological field.

Completion: $\hat{K} := \{\text{Cauchy sequences}\}/\{\text{Null sequences}\}$

is again a field (componentwise operations), $|\cdot|$ extends to $\hat{K}$: $\quad |(a_n)_{n\geq 0}| := \lim_{n\to\infty} |a_n|$

Exm: $\mathbb{R}$ is the completion of $\mathbb{Q}$ w.r.t. the „usual"

absolute value $|\cdot| = |\cdot|_\infty$ „archimedean abs. value of $\mathbb{Q}$".

p-adic absolute values: let $p \in \mathbb{P}$ ← set of prime numbers

Each $0 \neq a \in \mathbb{Q}$ has a repr. $a = p^e \frac{b}{c}$ with $e \in \mathbb{Z}$, $b, c \in \mathbb{Z}$, $p \nmid bc$.

e is unique, $v_p(a) := e$ (↙ p-adic valuation), $|a|_p := p^{-e} = p^{-v_p(a)}$ (p-adic absolute value)

$v_p(0) := \infty$, $|0|_p := p^{-\infty} := 0$.

Properties: $v_p(a) \in \mathbb{Z} \cup \{\infty\}$ $\qquad |a|_p \in \mathbb{R}_{\geq 0}$

$v_p(a) = \infty \iff a = 0 \iff |a|_p = 0$

$v_p(ab) = v_p(a) + v_p(b) \qquad |ab|_p = |a|_p |b|_p$

$v_p(a+b) \geq \min\{v_p(a), v_p(b)\} \Rightarrow |a+b|_p \leq \max\{|a|_p, |b|_p\} \leq |a| + |b|_p$

↑ ultrametric inequality

$\Rightarrow |\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is an absolute value. It is called non-archimedean since it satisfies the ultrametric inequality.

The completion $\mathbb{Q}_p$ is the field of p-adic numbers, $\mathbb{Q} \subseteq \mathbb{Q}_p$.

Digit representations:

$$\mathbb{Q}_p = \left\{ \sum_{i=-n}^{\infty} a_i p^i : \quad a_i \in \{0, \dots, p-1\},\ n \in \mathbb{Z} \right\}$$

↙ converges in p-adic topology!

Exm: in $\mathbb{Q}_2$: $-1 = \frac{1}{1-2} = \sum_{i=0}^{\infty} 2^i$ (all $a_i = 1$ for $i \geq 0$)

[note: $|2^i|_2 = 2^{-i}$

$\left|\sum_{i=M}^{N} 2^i\right|_2 \leq \max\{|2^i|_2 : M \leq i \leq N\} \leq 2^{-M} \to 0$ as $M \to \infty$!]

[Aside $\mathbb{Z}_p = \{\sum_{i=0}^{\infty} a_i p^i : a_i \in \{0, \dots, p-1\}\}$ is the subring of p-adic integers, $\mathbb{Z} \subseteq \mathbb{Z}_p$ (base-p expansion)

Can show: (1) $\mathbb{Q}_p$ is the quotient field of $\mathbb{Z}_p$

(2) $\mathbb{Z}_p \cong \varprojlim_{n \geq 0} \mathbb{Z}/p^n\mathbb{Z}$ (projective limit = colimit)]

Thm 7.4 (Ostrowski) Up to equivalence, $|\cdot|_\infty$, $|\cdot|_p$ ($p \in \mathbb{P}$) are the only non-trivial abs. values on $\mathbb{Q}$ (and these are inequivalent)

Here: $|\cdot|_1, |\cdot|_2 : K \to \mathbb{R}_{\geq 0}$ are equivalent $\Leftrightarrow$ they induce the same topology

$\Leftrightarrow \exists t > 0 : |\cdot|_1 = |\cdot|_2^t$.

Thm 7.5: $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ for all $p \in \mathbb{P}$

($\to$ Number Theory / Local Class Field Theory)

$\mathrm{Br}(\mathbb{R}) = \frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ $\quad (\frac{1}{2} + \mathbb{Z} = [\mathbb{H}],\ 0 + \mathbb{Z} = [\mathbb{R}])$

Thm 7.6: There is a SES

$$0 \to \mathrm{Br}(\mathbb{Q}) \xrightarrow{j} \bigoplus_{p \in \mathbb{P} \cup \{\infty\}} \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{f} \mathbb{Q}/\mathbb{Z} \to 0$$

Here: •) $j([R]) = ([R \otimes_{\mathbb{Q}} \mathbb{Q}_p])_p$

Fact: $R \otimes_{\mathbb{Q}} \mathbb{Q}_p = M_n(\mathbb{Q}_p)$ for all but fin. many p, so this really maps onto the direct sum

•) each $Br(\mathbb{Q}_p)$ can be identified w. $\mathbb{Q}/\mathbb{Z}$ (if $p \in \mathbb{P}$), resp. $\frac{1}{2}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$ $(p=\infty)$.

$$f : \bigoplus_p \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}, \quad (x_p + \mathbb{Z}) \longmapsto \Big(\sum_{p \in \mathbb{P}\cup\{\infty\}} x_p\Big) + \mathbb{Z}$$

•) Injectivity of j is the Hasse-Brauer-Noether-Albert Theorem (holds for K a number field, i.e. a finite field extension of $\mathbb{Q}$, with the „obvious modifications")

•) This is a local-global principle:

-) To understand a $\mathbb{Q}$-c.s.a. R, it suffices to understand it locally everywhere (only fin. many places non-trivial).

-) The $\mathbb{Q}/\mathbb{Z}$ on the right side describes the obstruction in passing back from local to global.

7.2 Relative Brauer Groups

Def: Let L/K be a field ext, $r_{L/K} : Br(K) \to Br(L)$, $[R] \mapsto [R \otimes_K L]$.
The relative Brauer group is $Br(L/K) := \ker(r_{L/K})$

I.e, $Br(L/K) \subseteq Br(K)$ consists of all $[R]$ s.t. R is split by L.

Thm 7.7: $Br(K) = \bigcup \{ Br(L/K) : L/K \text{ (finite) Galois extension} \}$

Proof: By C6.21, every K-CSA has a Galois splitting field. $\square$

Thm 7.8 If L/K is a field ext., $n=[L:K]<\infty$, and $[R]\in Br(L/K)$, then there exists a unique (up to iso) K-CSA S s.t. $R\sim S$, $L\subseteq S$ and $Z_S(L)=L$. In particular, L is a max. subfield of S.

Proof: Let $R\cong M_n(D)$, D div. algebra.

L splits R, hence D, so $L\otimes_K D\cong M_m(L)$, $m\geq 1$.

$m^2=\dim_L(L\otimes_K D)=\dim_K D$.

$L\otimes_K D$ is simple, let $V_{L\otimes_K D}$ be the unique simple right module.

$\Rightarrow (L\otimes_K D)\cong V^m$

$m\dim_K V=\dim_K(L\otimes_K D)=[L:K]m^2\Rightarrow \dim_K V=m[L:K]$.

Since the L- & D-actions on V commute with each other, there is a ring hom.
$$\varphi:\begin{cases} L\longrightarrow \operatorname{End}(V_D)=:S\\ \lambda\longmapsto (x\mapsto x\lambda)\end{cases}$$

L field $\Rightarrow\varphi$ injective, so wlog $L\subseteq S$.

$S\cong M_t(D)$, $t=\dim_D V=\dfrac{\dim_K V}{\dim_K D}=\dfrac{\cancel{m}[L:K]}{m^{\cancel{2}}}=\dfrac{[L:K]}{m}$

Note $S\sim R$ in $Br(K)$, $Z(S)=Z(D)=K$.

Show: $Z_S(L)=L$.

$[S:K]=\dfrac{[L:K]^2}{m^2}\overbrace{\dim_K D}^{=m^2}=[L:K]^2$

$\xRightarrow[\substack{S\ K\text{-CSA},\\ L\text{ simple}}]{T6.13}[L:K]=[Z_S(L):K]\xRightarrow{L\subseteq Z_S(L)} L=Z_S(L)$. $\square$

7.3 Factor System & Crossed Product Algebras

By T7.8, each class of $Br(L/K)$ w. L Galois has a „nice" repr. R w. $L \subseteq R$ a strict max. subfield ($Z_R(L)=L$).

<u>Fix:</u> L/K Galois extension, $G := Gal(L/K)$

<u>Recall:</u> $|G| = [L:K] = n$ (bec. L/K Galois),

Let R be a K-CSA w. L as strict max. subfield

$\overset{T6.10}{\Longrightarrow} \forall \sigma \in G \; \exists x_\sigma \in R \; \forall \lambda \in L: \quad x_\sigma \lambda x_\sigma^{-1} = \sigma(\lambda)$, i.e. $x_\sigma \lambda = \sigma(\lambda) x_\sigma$

<u>Lemma 7.9</u> (1) x_σ is unique up to a factor in $L^\times$

(2) $\forall \sigma, \tau \in G: \exists \gamma(\sigma,\tau) \in L^\times: \quad x_\sigma x_\tau = \gamma(\sigma,\tau) x_{\sigma\tau}$ (1)

<u>Proof:</u> (1) If $x_\sigma \lambda x_\sigma^{-1} = x'_\sigma \lambda (x'_\sigma)^{-1} \quad \forall \lambda \in L$

$\Rightarrow (x'_\sigma)^{-1} x_\sigma \lambda = \lambda (x'_\sigma)^{-1} x_\sigma \Rightarrow x'^{-1}_\sigma x_\sigma \in Z_R(L) = L.$

(2) $x_\sigma x_\tau \lambda x_\tau^{-1} x_\sigma^{-1} = \sigma\tau(\lambda)$; (1) implies the claim. $\square$

<u>Lemma 7.10:</u> $(x_\sigma)_{\sigma \in G}$ is an L-basis of R

<u>Proof:</u> Since $|G| = [L:K] = [R:L]$, it suffices to show linear independence. Suppose $\sum_{\sigma \in J}' \alpha_\sigma x_\sigma = 0$ (*) with $0 \neq \alpha_\sigma \in L$,

and $\emptyset \neq J$ minimal s.t. such a lin. dependence exists. ($\Rightarrow |J| \geq 2$)

Fix $\tau \in J$. $\forall \lambda \in L: \quad 0 = \sum_{\sigma \in J}' \alpha_\sigma x_\sigma \lambda = \sum_{\sigma \in J}' \alpha_\sigma \sigma(\lambda) x_\sigma$

and $\quad 0 \overset{\tau(\lambda)\cdot (*)}{=} \sum_{\sigma \in J}' \alpha_\sigma \tau(\lambda) x_\sigma$

$$\Rightarrow \quad 0 = \sum_{\sigma \in J \setminus \{\tau\}}' \alpha_\sigma (\sigma(\lambda) - \tau(\lambda)) x_\sigma. \quad \text{Because } \sigma \neq \tau, \ \exists \lambda \in L^\times$$

s.t. this lin. combination has nonzero coeffs $\lightning$ minimality of S. $\square$

So $\gamma: G \times G \to L^\times$ determines the algebra R.

R associative $\rightarrow$ $\forall \sigma, \tau, \varsigma \in G$: $\quad x_\varsigma(x_\sigma x_\tau) = (x_\varsigma x_\sigma) x_\tau$

$$x_\varsigma(x_\sigma x_\tau) = x_\varsigma(\gamma(\sigma,\tau)\, x_{\sigma\tau}) = \varsigma(\gamma(\sigma,\tau))\, x_\varsigma x_{\sigma\tau} =$$
$$= \varsigma(\gamma(\sigma,\tau))\, \gamma(\varsigma, \sigma\tau)\, x_{\varsigma\sigma\tau}$$

$$(x_\varsigma x_\sigma) x_\tau = \gamma(\varsigma,\sigma)\, x_{\varsigma\sigma} x_\tau = \gamma(\varsigma,\sigma)\, \gamma(\varsigma\sigma,\tau)\, x_{\varsigma\sigma\tau}$$

$$\Rightarrow \quad \boxed{\varsigma(\gamma(\sigma,\tau))\, \gamma(\varsigma,\sigma\tau) = \gamma(\varsigma,\sigma)\, \gamma(\varsigma\sigma,\tau)} \quad (*)$$

<u>Def:</u> A map $\gamma: G \times G \to L^\times$ is a factor system or 2-cocycle (of G with values in $L^\times$), if it satisfies $(*)$

<u>Prop 7.11</u> Let R be an L-vector space with basis $(x_\sigma)_{\sigma \in G}$.

and $\gamma: G \times G \to L^\times$. Then the multiplication

$$\Big(\sum_{\sigma \in G}' \alpha_\sigma x_\sigma\Big) \cdot \Big(\sum_{\tau \in G}' \beta_\tau x_\tau\Big) := \sum_{\sigma,\tau \in G}' \alpha_\sigma\, \sigma(\beta_\tau)\, \gamma(\sigma,\tau)\, x_{\sigma\tau}.$$

defines a K-algebra structure on $R \Leftrightarrow \gamma$ is a 2-cocycle.

<u>Proof.</u> „$\Rightarrow$" By discussion before the definition

„$\Leftarrow$" Check ring axioms: $\forall r, s, t$:

(i) $r(s+t) = rs + rt$, $(r+s)t = rt + st$ (Straightforward)

(ii) with $1 = \gamma(id,id)^{-1} x_{id}$: $r1 = 1r = r$.

$$(\alpha_\sigma x_\sigma)\, \gamma(id,id)^{-1} x_{id} = \alpha_\sigma\, \sigma(\gamma(id,id)^{-1})\, \gamma(\sigma,id)\, x_\sigma = \alpha_\sigma x_\sigma$$

By $\circledast$: $\sigma(\gamma(id,id))\, \cancel{\gamma(\sigma,id)} = \gamma(\sigma,id)\, \cancel{\gamma(\sigma,id)}$

$(\varsigma \leftarrow \sigma,\ \sigma = \tau \leftarrow id)$

$$\gamma(id,id)^{-1} x_{id}\, (\alpha_\sigma x_\sigma) = \gamma(id,id)^{-1} \alpha_\sigma\, \gamma(id,\sigma)\, x_\sigma = x_\sigma \alpha_\sigma.$$

$$\circledast \Rightarrow \quad \gamma(id,\sigma)\, \gamma(id,\sigma) = \gamma(id,id)\, \gamma(id,\sigma)$$

(iii): $(a_\varsigma x_\varsigma)(b_\sigma x_\sigma\, c_\tau x_\tau) = a_\varsigma x_\varsigma\, (b_\sigma\, \sigma(c_\tau)\, \gamma(\sigma,\tau)\, x_{\sigma\tau})$

$$= a_\varsigma\, \varsigma(b_\sigma)\, \varsigma(\sigma(c_\tau))\, \underbrace{\varsigma(\gamma(\sigma,\tau))\, \gamma(\varsigma,\sigma\tau)}\, x_{\varsigma\sigma\tau}$$

$$\underset{\circledast}{=} a_\varsigma\, \varsigma(b_\sigma)\, \varsigma(\sigma(c_\tau))\, \gamma(\varsigma,\sigma)\, \gamma(\varsigma\sigma,\tau)\, x_{\varsigma\sigma\tau}$$

$$= a_\varsigma\, \varsigma(b_\sigma)\, \gamma(\varsigma,\sigma)\, x_{\varsigma\sigma}\, c_\tau x_\tau = (a_\varsigma x_\varsigma\, b_\sigma x_\sigma)\, c_\tau x_\tau.$$

K is central because $\sigma|_K = id \ \forall \sigma \in G$. $\square$

Def: The algebra R, defined as in P7.11, with γ a 2-cocycle, is the crossed product algebra of L and G w.r.t. γ.

Notation: (L, G, γ)

Thm 7.12 $R = (L, G, \gamma)$ is a K-CSA, $L \subseteq R$ a strict max. subfield.

Proof: $L \hookrightarrow R$ via $\lambda \mapsto \lambda \cdot 1_R$, $\quad 1_R = \gamma(id,id)^{-1} x_{id}$

$Z_R(L) = L$: $\quad \sum'_{\sigma \in G} \alpha_\sigma x_\sigma \in Z_R(L)$

$$\Leftrightarrow \forall \lambda \in L: \quad \lambda \sum'_{\sigma \in G} \alpha_\sigma x_\sigma = \Big(\sum'_{\sigma \in G} \alpha_\sigma x_\sigma\Big) \lambda$$

$$\Leftrightarrow \forall \lambda \in L\ \forall \sigma \in G: \quad \lambda \alpha_\sigma = \alpha_\sigma\, \sigma(\lambda)$$

If $\alpha_\sigma \neq 0$, then $\lambda = \sigma(\lambda)$, i.e. $\sigma = id_L$ $\Rightarrow$ only $\alpha_{id} \neq 0$.

$\rightarrow Z_R(L) = L x_{id} = L$. $\quad$ $Z(R) = K$: $Z(R) \subseteq Z_R(L) = L$; now easy to check $Z(R) = K$.

R is simple: let $I \trianglelefteq R$

$L^\times = L \setminus \{0\} \subseteq R^\times \Rightarrow L \cap I = 0.$

$\Rightarrow L$ embeds into R/I.

$(x_\sigma + I)_{\sigma \in G}$ is lin. independent (as in L7.10)

$\Rightarrow \dim_L R/I = |G| = \dim_L R \Rightarrow I = \underline{0}.$ $\square$